PCT/AU2004/001083

Patent Office
Canberra

I, JULIE BILLINGSLEY, TEAM LEADER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. 2003904317 for a patent by SECURICOM (NSW) PTY LTD as filed on 13 August 2003.

WITNESS my hand this
Twenty-third day of August 2004

J. Billingsley

JULIE BILLINGSLEY
TEAM LEADER EXAMINATION
SUPPORT AND SALES

S&F Ref: 642682

AUSTRALIA

Patents Act 1990

PROVISIONAL SPECIFICATION FOR THE INVENTION ENTITLED:

Remote Entry System

Name and Address of Applicant:

Securicom (NSW) Pty Ltd, an Australian company, ACN 053 874 089, of PO Box 124, Ramsgate, New South Wales, 2217, Australia

Name of Inventor:

Christopher John Burke

This invention is best described in the following statement:

REMOTE ENTRY SYSTEM

Field of the Invention

The present invention relates to secure access systems and, in particular, to systems using wireless transmission of security code information.

Background

Fig. 1 shows a prior art arrangement for providing secure access. A user 401 makes a request, as depicted by an arrow 402, directed to a code entry module 403. The module 403 is typically mounted on the external jamb of a secure door. The request 402 is typically a secure code of some type which is compatible with the code entry module 403. Thus, for example, the request 402 can be a sequence of secret numbers directed to a keypad 403. Alternately, the request 402 can be a biometric signal from the user 401 directed to a corresponding biometric sensor 403. One example of a biometric signal is a fingerprint.

The code entry module 403 conveys the request 402 by sending a corresponding signal, as depicted by an arrow 404, to a controller 405 which is typically situated in a remote or inaccessible place. The controller 405 authenticates the security information provided by the user 401 by interrogating a database 407 as depicted by an arrow 406. If the user 401 is authenticated, and has the appropriate access privileges, then the controller 405 sends an access signal, as depicted by an arrow 408, to a device 409 in order to provide the desired access. The device 409 can, for example, be the locking mechanism of a secure door, or can be an electronic lock on a personal computer (PC) which the user 401 desires to access.

A proximity card can also be used to emit the request 402, in which case the code entry module 403 has appropriate functionality.

Although the request 402 can be made secure, either by increasing the number of secret digits or by using a biometric system, the communication infrastructure in Fig. 1 is

typically less secure. The infrastructure 400 is generally hardwired, with the code entry module 403 generally being mounted on the outside jamb of a secured door. In such a situation, the signal path 404 can be over a significant distance in order to reach the controller 405. The path 404 represents one weak point in the security system 400, providing an unauthorised person with relatively easy access to the information being transmitted between the code entry module 403 and the controller 405. Such an unauthorised person can, given this physical access, decipher the communicated information between the code entry module 403 and the controller 405. This captured information can be deciphered, replayed in order to gain the access which rightfully belongs to the user 401, or to enable modification for other subversive purposes.

Current systems as depicted in Fig. 1 utilise a communication protocol called "Wiegand" for communication between the code entry module 403 and the controller 405. The Wiegand protocol is a simple one-way data protocol that can be modified by increasing or decreasing the bit count to ensure uniqueness of the protocol among different security companies. The Wiegand protocol does not secure the information being sent between the code entry module 403 and the controller 405.

More advanced protocols such as RS 485 have been used in order to overcome the vulnerability of the Wiegand protocol over the long distance route 404. RS 485 is a duplex protocol offering encryption capabilities at both the transmitting and receiving ends, ie. the code entry module 403 and the controller 405 respectively in the present case. The length of the path 404 nonetheless provides an attack point for the unauthorised person.

Due to the cost and complexity of re-wiring buildings and facilities, security companies often make use of existing communication cabling when installing and/or upgraded security systems, thereby maintaining the vulnerability described above.

Summary

It is an object of the present invention to substantially overcome, or at least ameliorate, one or more disadvantages of existing arrangements.

Disclosed are arrangements which seek to address the above problems by replacing the vulnerable wired path 404 with a strongly encrypted wireless path between the code entry module and the controller, and by incorporating biometric authentication at the code entry module 403.

According to a first aspect of the present invention, there is provided a system for providing secure access, the system comprising:

a biometric sensor for authenticating the identity of a user;

a transmitter for transmitting information using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and

a control panel for receiving the information and for providing the secure access requested.

Other aspects of the invention are also disclosed.

Brief Description of the Drawings

Some aspects of the prior art and one or more embodiments of the present invention are described with reference to the drawings, in which:

Fig. 1 shows a prior art arrangement for providing secure access;

Fig. 2 is a functional block diagram of an arrangement for providing secure access according to the present disclosure;

Fig. 3 shows the method of operation of the remote control module of Fig. 2;

Fig. 4 shows the method of operation of the (fixed) control device of Fig. 2; and

Fig. 5 shows incorporation of a protocol converter into the arrangement of Fig. 2.

Detailed Description including Best Mode

It is to be noted that the discussions contained in the "Background" section relating to prior art arrangements relate to discussions of documents or devices which

form public knowledge through their respective publication and/or use. Such should not be interpreted as a representation by the present inventor(s) or patent applicant that such documents or devices in any way form part of the common general knowledge in the art.

Where reference is made in any one or more of the accompanying drawings to steps and/or features, which have the same reference numerals, those steps and/or features have for the purposes of this description the same function(s) or operation(s), unless the contrary intention appears.

Fig. 2 is a functional block diagram of an arrangement for providing secure access according to the present disclosure. A user 101 makes a request, as depicted by an arrow 102, to a code entry module 103. The code entry module 103 is a biometric sensor and the request 102 takes a form which corresponds to the nature of the sensor 103. Thus, for example, if the sensor 103 is a fingerprint sensor, then the request 102 typically takes the form of a thumb press on a sensor panel (not shown) on the code entry module 103.

The code entry module 103 interrogates, as depicted by an arrow 104, a user identity database 105. Thus for example if the request 102 is the thumb press on the biometric sensor panel then the user database 105 contains biometric signatures for authorised users against which the request 102 can be authenticated. If the identity of the user 101 is authenticated successfully, then the code entry module 103 sends a signal 106 to a controller/transmitter 107. The controller/transmitter 107 checks, as depicted by an arrow 112, the current rolling code in a database 113. The controller 107 then updates the code and sends the updated code as depicted by an arrow 108 to a controller 109. The rolling code protocol offers non-replay encrypted communication.

The controller 109 tests the rolling code received at 108 against the most recent rolling code which has been stored in a database 115, this testing being depicted by an arrow 114. If the incoming rolling code 108 is found to be legitimate, then the controller 109 sends a command, as depicted by an arrow 110, to a controlled item 111. The

controlled item 111 can be a door locking mechanism on a secure door, or an electronic key circuit in a personal computer (PC) that is to be accessed by the user 101. It is noted that the controller 109 contains a receiver 118 that receives the transmitted signal 108 and converts it into a form that the controller 109 can use.

The arrangement in Fig. 2 has been described for the case in which the secure code 108 used between the sub-system116 and 117 is based upon the rolling code. It is noted that this is merely one arrangement, and other secure codes can equally be used.

Rolling codes provide a substantially non-replayable non-repeatable and encrypted radio frequency data communications scheme for secure messaging. These codes use inherently secure protocols and serial number ciphering techniques which in the present disclosure hide the clear text values required for authentication between the key fob (transmitter) sub-system 116 and the receiver/controller 118/109.

Rolling codes use a different code variant each time the transmission 108 occurs. This is achieved by encrypting the data from the controller 107 with a mathematical algorithm, and ensuring that successive transmissions 108 are modified using a code and/or a look-up table known to both the transmitter sub-system 116 and the receiver sub-system 117. Using this approach successive transmissions are modified, resulting in a non-repeatable data transfer, even if the information from the controller 107 remains the same. The modification of the code 108 for each transmission significantly reduces the likelihood that an intruder can access the information replay the information to thereby gain entry at some later time.

The sub-system in Fig. 2 falling to the left hand side, as depicted by an arrow 116, of a dashed line 119 can be implemented in a number of different forms. The sub-system 116 can for example be incorporated into a remote fob (which is a small portable device carried by the user 101), or alternately can be mounted in a protected enclosure on the outside jamb of a secured door. The sub-system 116 communicates with the sub-

system 117 on the right hand side of the dashed line 119 via the wireless communication channel 108. The sub-system 117 is typically located in an inaccessible area such as a hidden roof space or alternately in a suitable protected area such as an armoured cupboard. The location of the sub-system 117 must of course be consistent with reliable reception of the wireless signal 108.

The biometric signature database 105 is shown in Fig. 2 to be part of the sub-system 116. However, in an alternate arrangement, the biometric signature database 105 can be located in the sub-system 117, in which case the communication 104 between the biometric sensor 103 and the signature database 105 can also be performed over a secure wireless communication channel such as 108. In the event that the secure access system is being applied to providing secure access to a PC, then the secured PC can store the biometric signature of the authorised user in internal memory, and the PC can be integrated into the sub-system 117 of Fig. 1.

In the event that the sub-system 116 is implemented as a remote fob, the combination of the biometric verification and the strongly encrypted wireless communication provides a particularly significant advantage over current systems. The remote key fob arrangement allows easy installation, since the wired communication path 404 (see Fig. 1) is avoided. Other existing wiring elements of the present systems 400 can be used where appropriate. When the sub-system 116 is implemented as a remote fob, the fob incorporates the biometric (eg fingerprint) authentication arrangement, in which case only one biometric signature is stored in the fob. This arrangement reduces the requirements on the central database 115. Once the key fob authenticates the user through biometric signature (eg fingerprint) verification, the rolling code 108 is transmitted to the controller 109 for authorisation of the user for that location at that time.

In addition to authenticating the user 101 the biometric sensor 103 in conjunction with the controller 107 can also check other access privileges of the user 101. These

access privileges can be contained in the database 105 which be located either locally in the remote key fob, or in the sub-system 117 as previously described. In one example, Tom Smith can firstly be authenticated as Tom Smith using the thumb press by Tom on the biometric sensor panel (not shown). After Tom's personal biometric identity is authenticated, the sub-system 116 can check if Tom Smith is in fact allowed to use the particular door secured by the device 111 on weekends. Thus the security screening offered by the described arrangement can range from simple authentication of the user's identity, to more comprehensive access privilege screening.

The incorporation of the biometric sensor 103 into a remote key fob also means that if the user 101 loses the remote key fob, the user need not be concerned that someone else can use it. Since the finder of the lost key fob will not be able to have his or her biometric signal authenticated by the biometric sensor 103, the lost key fob is useless to anyone apart from the rightful user 101.

The sub-system 116 is preferably fabricated in the form of a single integrated circuit (IC) to reduce the possibility of an authorised person bypassing the biometric sensor 103 and directly forcing the controller 107 to emit the rolling code 108.

Fig. 3 shows the method of operation of the remote control module (ie the sub-system 116) of Fig. 2. The method 200 commences with a testing step 201 in which the biometric sensor 103 checks whether a biometric signal 102 is being received. If this is not the case, then the method 200 is directed in accordance with an NO arrow back to the step 201 in a loop. If, on the other hand, the biometric signal 102 has been received, then the method 200 is directed in accordance with a YES arrow to a step 202. The step 202 compares the received biometric signal 102 with information in the biometric signature database 105 in order to ensure that the biometric signal received 102 is that of the rightful user 101 of the sub-system 116.

A subsequent testing step 203 checks whether the comparison in the step 202 yields the desired authentication. If the biometric signature matching is authenticated, then the process 200 is directed in accordance with a YES arrow to a step 204. The step 204 enables the user 101 to select a control option by providing one or more additional signals (not shown) to the controller 107. Thus for example the control option could enable the user 101 to access one of a number of secure doors after his or her identity has been authenticated in the step 203. In the subsequent step 205 the controller 107 sends the appropriate control signal 108 to the controller 109. The process 200 is then directed in accordance with an arrow 206 back to the step 201.

Thus for example the sub-system 116 can be provided with a single biometric sensor 103 which enables the user 101 to select one of four door entry control signals by means of separate buttons on the controller 107 (not shown). This would enable the user 101, after authentication by the biometric sensor 103 and the controller 107 to obtain access to any one of the aforementioned for secure doors.

Returning to the testing step 203, if the signature comparison indicates that the biometric signal 102 is not authentic, and has thus not been received from the proper user, then the process 200 is directed in accordance with a NO arrow back to the step 201. In an alternate arrangement, the NO arrow from the step 203 could lead to a disabling step which would disable further operation of the sub-system 116, either immediately upon receipt of the incorrect biometric signal 102, or after a number of attempts to provide the correct biometric signal 102.

Fig. 4 shows the method of operation of the control sub-system 117 of Fig. 2. The method 300 commences with a testing step 301 which continuously checks whether the control signal 108 has been received from 107. The step 301 is performed by the controller 109. As long as the control signal 108 is not received the process 300 is directed in accordance with a NO arrow in a looping manner back to the step 301. When

the control signal 108 is received, the process 300 is directed from the step 301 by means of a YES arrow to a step 302. In the step 302, the controller 109 compares the rolling code received by means of the control signal 108 with a reference code in the database 115. A subsequent testing step 303 is performed by the controller 109. In the step 303 if the code received on the control signal 108 is successfully matched against the reference code in the database 115 then the process 300 is directed in accordance with a YES arrow to a step 304.

In the step 304 the controller 109 sends the control signal 110 to the controlled item 111 (for example opening the secured door). The process 300 is then directed from the step 304 as depicted by an arrow 305 back to the step 301. Returning to the testing step 303 if the code received on the control signal 108 is not successfully matched against the reference code in the database 115 by the controller 109 then the process 300 is directed from the step 303 in accordance with a NO arrow back to the step 301.

As was described in regard to Fig. 3, in an alternate arrangement, the process 300 could be directed, if the code match is negative, from the step 303 to a disabling step which would disable the sub-system 117 if the incorrect code where received once or a number of times.

Fig. 5 shows incorporation of a protocol converter into the arrangement of Fig. 2. In the arrangement of Fig. 2 the receiver 118 in the controller 109 is able to directly receive and process the rolling code 108 in a manner as to provide the necessary information to the controller 109. Fig. 5 shows how existing controllers which use Wiegand input signalling can be used in the disclosed arrangement when alarm systems are upgraded. Fig. 5 shows how the incoming signal 108 is received by the receiver 118 as is the case in Fig. 2. In Fig. 5 however the receiver 118 provides the received rolling code 108, as depicted by an arrow 503, to a rolling code/Wiegand protocol converter 501. The converter 501 converts the incoming rolling code 502 to a form, as depicted by an

arrow 504, that can be used when the controller 109 is designed to handle Wiegand protocol incoming signals. Therefore, the converted incoming signal 504 is in the Wiegand format.

The converter 501 uses a microprocessor-based arrangement running software code to process the incoming rolling code information 503 and decode this information 503 to clear text form. The converter 501 converts this clear text to a Wiegand variable bit-length data stream. In Fig. 2, the receiver 118 performs the conversion of the incoming rolling code signal 108 to clear text which enables the controller 109 to identify the serial number of the originating key fob sub-system 116 to enable the access rights of the user to be verified.

Further to the Wiegand conversion arrangement, the protocol converter 501 approach can be adapted to convert between the incoming rolling code 502 (or any other appropriate secure code) to any other convenient protocol used by the controller 109.

The advantage of the rolling code/Wiegand converter 501 is that security system upgrades can be made without replacing Wiegand compatible controller 109. Accordingly, existing systems as are described in Fig. 1 can be upgraded by replacing the code entry module 403 and the transmission path 404, leaving the other components of the system 400 (ie., the controller 405, the code database 407, and the controlled item 409, together with existing wiring 408 and 406), largely intact. Minor modifications might however be necessary. When upgrading systems in this manner, the sub-system 116 can either be used in a remote fob configuration, or can be placed in a secure housing on an external door jamb.

From a practical perspective, incorporating the protocol converter 501 into an existing controller 109 would require direct wiring of the converter 501 into the secure controller 109 housing.

Industrial Applicability

It is apparent from the above that the arrangements described are applicable to the security industry.

The foregoing describes only some embodiments of the present invention, and modifications and/or changes can be made thereto without departing from the scope and spirit of the invention, the embodiments being illustrative and not restrictive.

The system 100 can also be used to provide authorised access to lighting systems, building control devices, exterior or remote devices such as air compressors and so on. The concept of "secure access" is thus extendible beyond mere access to restricted physical areas.

AUSTRALIA ONLY

In the context of this specification, the word "comprising" means "including principally but not necessarily solely" or "having" or "including", and not "consisting only of". Variations of the word "comprising", such as "comprise" and "comprises" have correspondingly varied meanings.

The claims defining the invention are as follows:

1. A system for providing secure access, the system comprising:

a biometric sensor for authenticating the identity of a user;

a transmitter for transmitting information using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and

a control panel for receiving the information and for providing the secure access requested.

2. A system according to claim 1 wherein the control panel includes a converter for receiving the secure wireless signal and for outputting the information.

3. A system according to claim 1, wherein the biometric sensor authenticates the identity of the user by comparing a biometric input from the user with a biometric signature for the user in a biometric database.

4. A system according to claim 3, wherein the biometric sensor, the biometric database, and the transmitter are located in a remote fob.

5. A system according to claim 1, wherein the secure wireless signal comprises an RF carrier and a rolling code.

6. A system according to claim 2, wherein the secure wireless signal comprises an RF carrier and a rolling code, and the converter converts the rolling code to the Wiegand protocol.

7. A system for providing secure access substantially as described herein with reference to accompanying Figs. 2-5.

8. A method for providing secure access substantially as described herein with reference to accompanying Figs. 2-5.

DATED this 13th Day of August 2003

SECURICOM (NSW) PTY LTD

Patent Attorneys for the Applicant

SPRUSON&FERGUSON

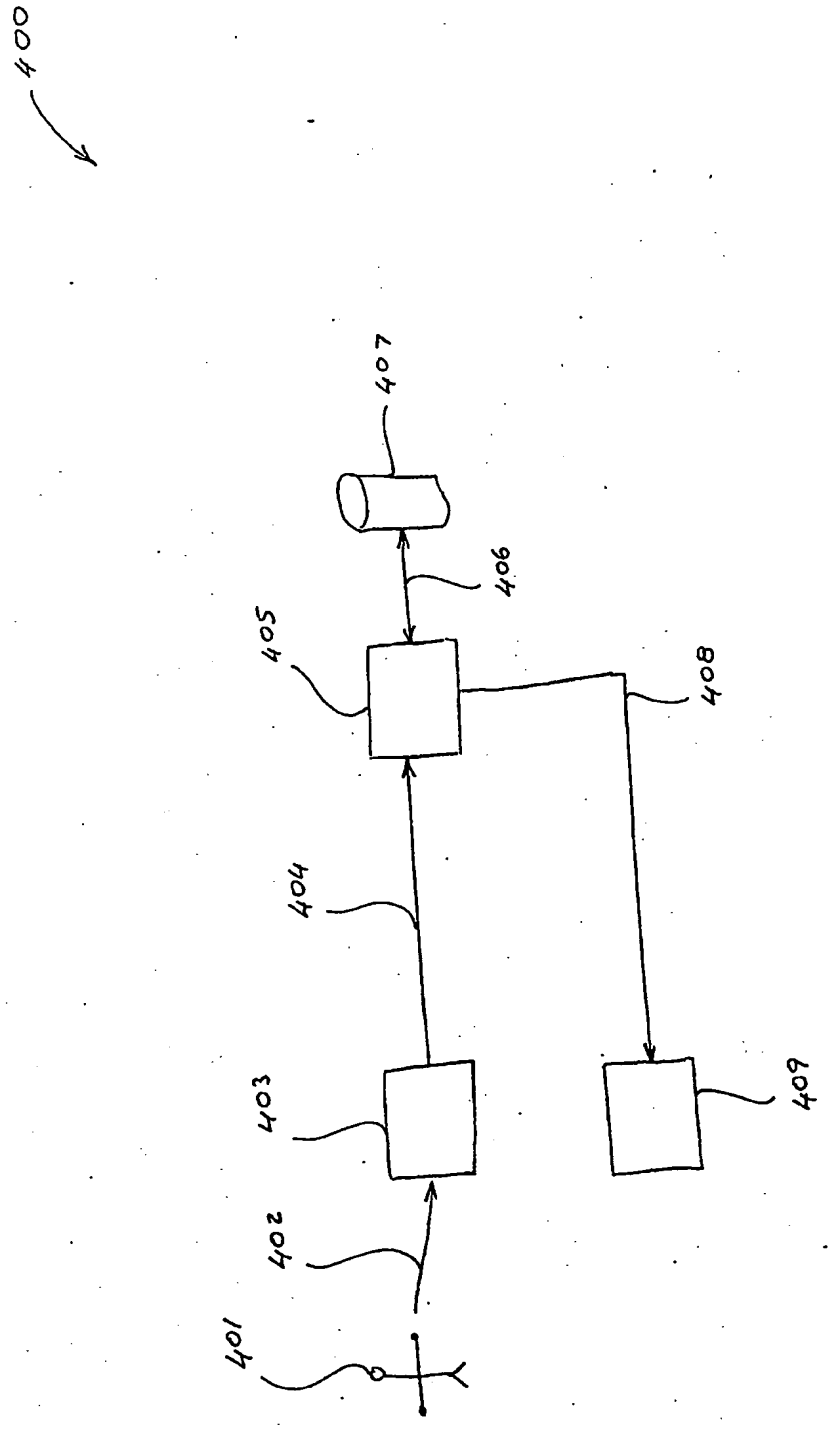

Fig. 1
(prior art)

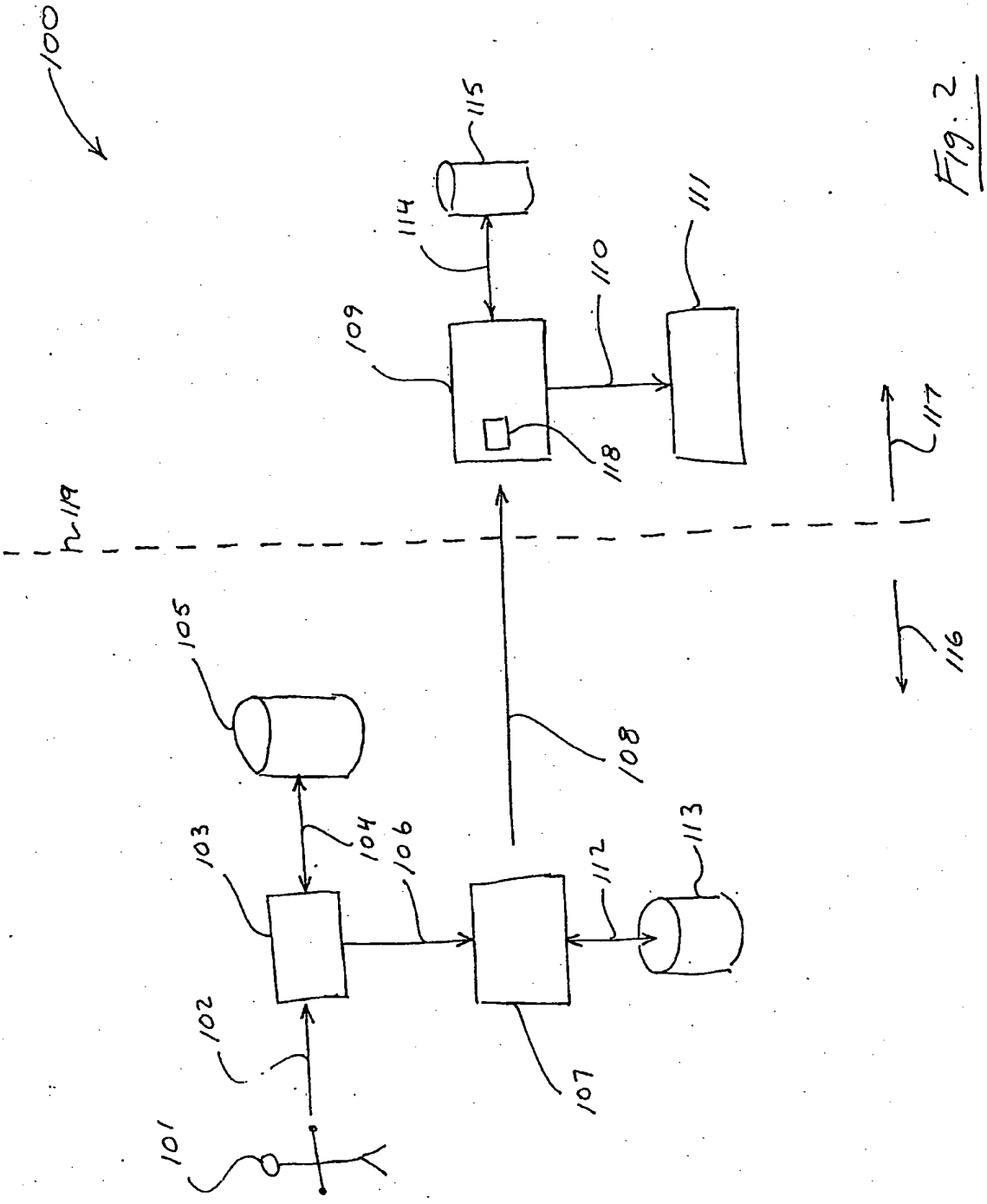
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119

Fig. 2

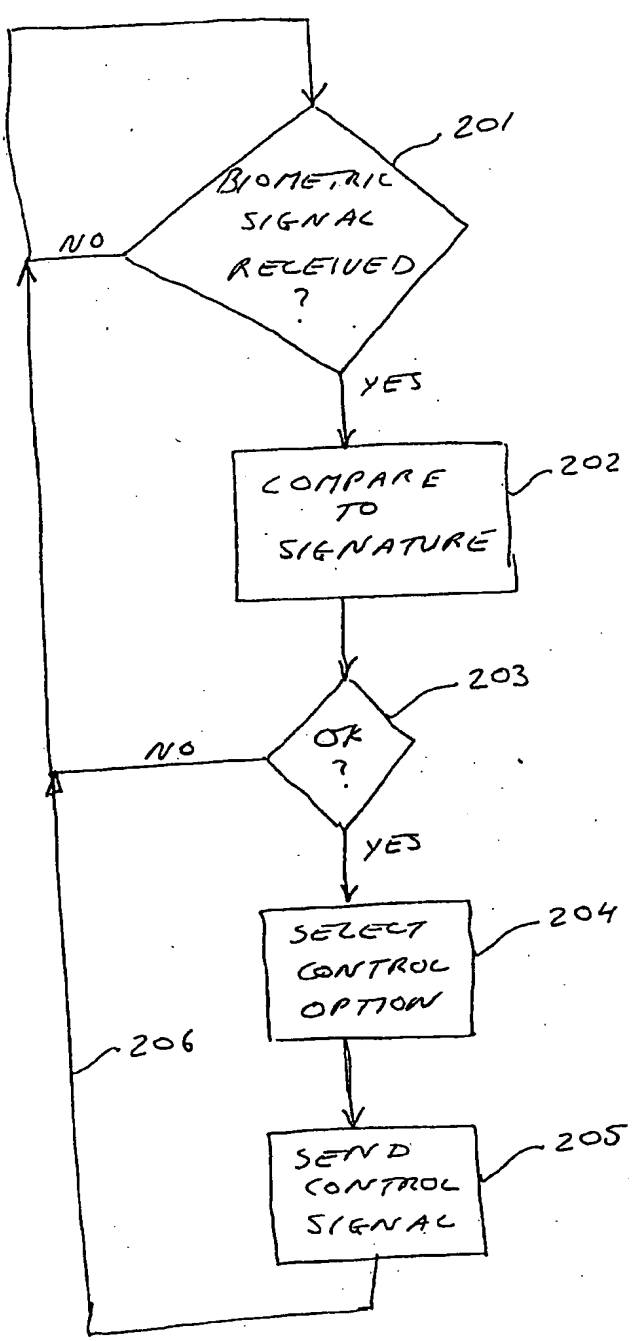
200
201
BIOMETRIC SIGNAL RECEIVED ?
NO
YES
202
COMPARE TO SIGNATURE
203
OK ?
NO
YES
204
SELECT CONTROL OPTION
205
SEND CONTROL SIGNAL
206

Fig. 3

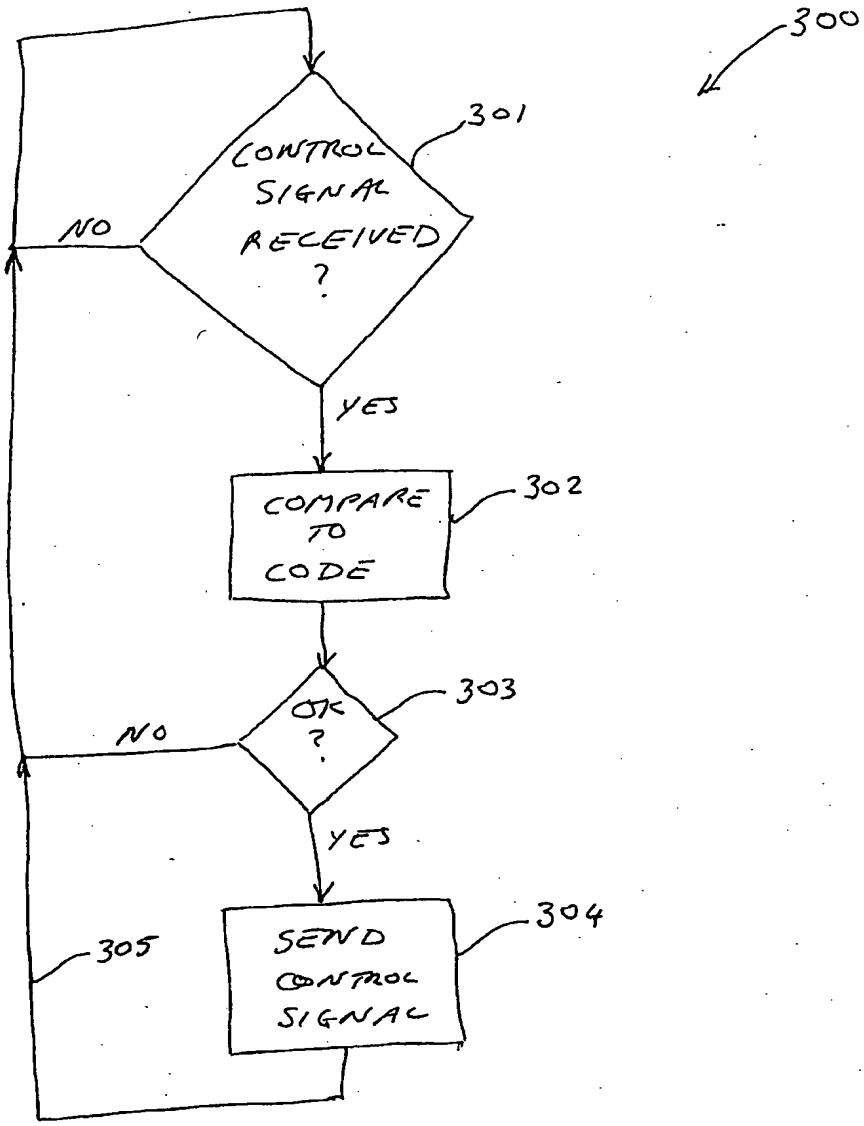
300
301
CONTROL SIGNAL RECEIVED ?
NO
YES
302
COMPARE TO CODE
303
OK ?
NO
YES
304
SEND CONTROL SIGNAL
305

Fig. 4

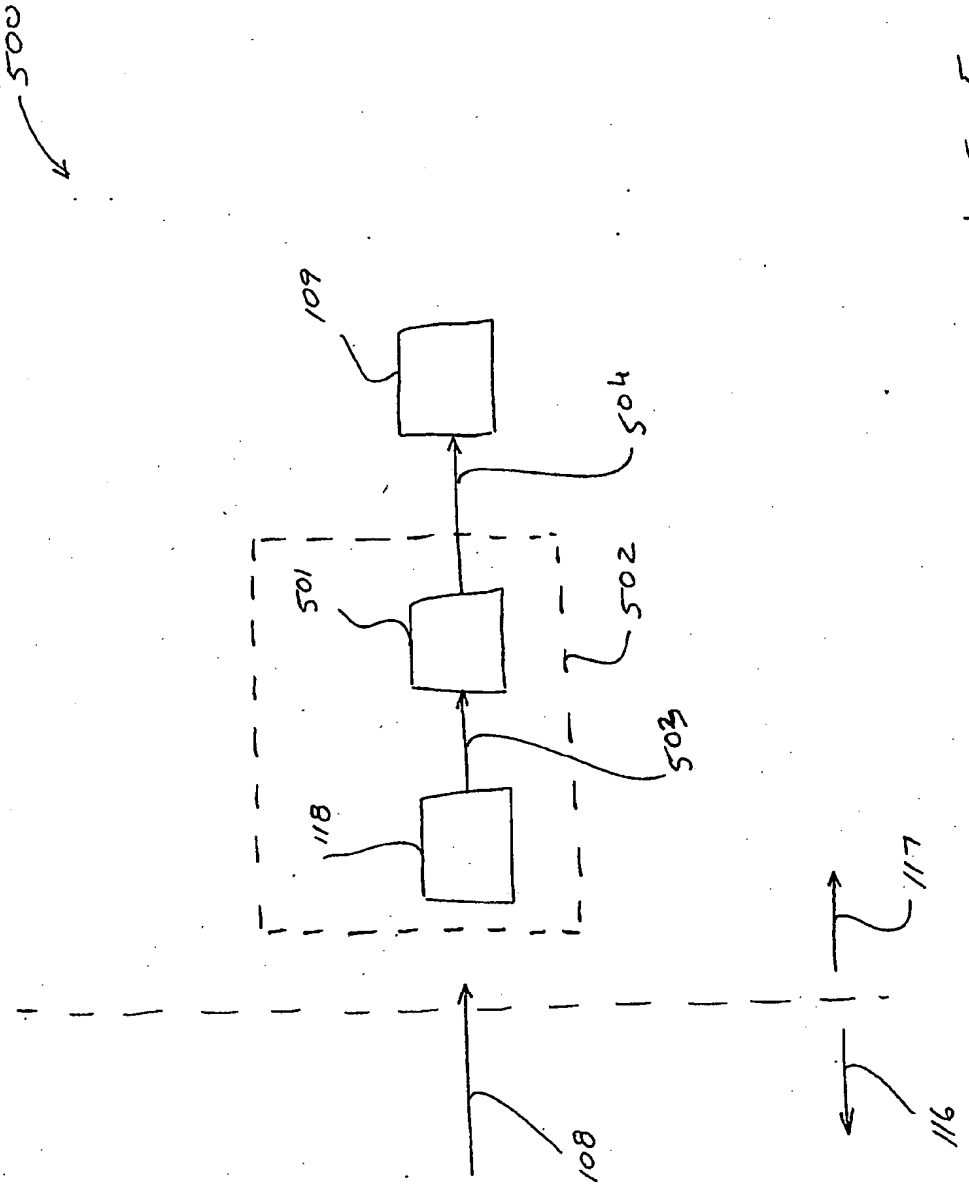

Fig. 5